Available online at www.sciencedirect.com

ScienceDirect

Linear Algebra and its Applications 430 (2009) 1778–1789

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Galois theory and linear algebra☆

Rod Gow*, Rachel Quinlan

School of Mathematical Sciences, University College, Belfield, Dublin 4, Ireland
Department of Mathematics, National University of Ireland, Galway, Ireland

Received 11 February 2008; accepted 23 June 2008
Available online 19 August 2008
Submitted by R. Loewy

Dedicated to Tom Laffey on the occasion of his 65th birthday, and recalling many years of friendship and fruitful collaboration.

Abstract

Let K be a field admitting a Galois extension L of degree n with Galois group G. Artin's lemma on the independence of characters implies that the algebra of K-linear endomorphisms of L is identical with the set of L-linear combinations of the elements of G. This paper examines some consequences of this description of endomorphisms. We provide a characterization of the rank 1 endomorphisms and describe the matrix-theoretic trace of an endomorphism in terms of the field-theoretic trace. We also investigate in greater detail those endomorphisms annihilating a K-subspace in the case when G is cyclic.

AMS classification: 12F10; 15A03; 15A04

Keywords: Field; Galois extension; Cyclic extension; Galois group; Hyperplane; Endomorphism annihilating a subspace; Polynomial

1. Introduction

Let K be a field and let L be a Galois extension of K of finite degree n. Let G denote the Galois group of L over K. We may consider L to be a vector space of dimension n over K and it serves as a model for any such n-dimensional vector space. However, the Galois nature of the extension

☆ Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.
* Corresponding author. Address: School of Mathematical Sciences, University College, Belfield, Dublin 4, Ireland.
E-mail addresses: rod.gow@ucd.ie (R. Gow), rachel.quinlan@nuigalway.ie (R. Quinlan).

0024-3795/$ - see front matter
doi:10.1016/j.laa.2008.06.030

enriches the vector space structure and enables us to carry out constructions, especially related to K-linear transformations, which we could not achieve without the additional field-theoretic apparatus.

Let $\mathrm{End}_K(L)$ denote the algebra of all K-linear endomorphisms of L. $\mathrm{End}_K(L)$ is of course a vector space of dimension n^2 over K and we may identify it with the algebra of $n \times n$ matrices with entries in K. Our first main result of this paper uses Artin's lemma on the independence of characters to show that $\mathrm{End}_K(L)$ equals the set of L-linear combinations of elements of G. We remark here that the K-linear independence of the Galois automorphisms is frequently used in the development of basic Galois theory but the full force of the fact that these automorphisms are actually linearly independent over L is not exploited in the same way. The main purpose of this paper is to explore some consequences of this identification of $\mathrm{End}_K(L)$ with the set of L-linear combinations of elements of G.

2. The K-linear endomorphisms of L and Galois automorphisms

We continue to use the notation introduced above. Let

$$G = \{\sigma_1, \ldots, \sigma_n\},$$

where we assume that $\sigma_1 = 1$ is the identity element, and let $\lambda_1, \ldots, \lambda_n$ be elements of L. We define a function $\tau : L \to L$ by setting

$$\tau(x) = \lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x)$$

for all $x \in L$, and we write correspondingly

$$\tau = \lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n.$$

It is easy to see that τ is in $\mathrm{End}_K(L)$ and we claim that every element of $\mathrm{End}_K(L)$ arises in this way for unique elements $\lambda_1, \ldots, \lambda_n$ in L.

Theorem 1. *Each element of* $\mathrm{End}_K(L)$ *is expressible in the form*

$$\lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n$$

for unique elements $\lambda_1, \ldots, \lambda_n$ *in* L.

Proof. Let E denote the set of all endomorphisms of L of the form above. E is clearly a K-subspace of $\mathrm{End}_K(L)$ and we will show that it equals $\mathrm{End}_K(L)$ by exhibiting n^2 elements of E that are linearly independent over K. Let $\{\mu_1, \ldots, \mu_n\}$ be a K-basis for L. Consider the n^2 elements $\mu_i\sigma_j$ of E, where $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$. Suppose that we have a dependence relation

$$\sum_{1 \leqslant i,j \leqslant n} \alpha_{ij}\mu_i\sigma_j = 0,$$

where the α_{ij} are in K. Then we obtain

$$\sum_{j=1}^{n} \lambda_j\sigma_j = 0,$$

where

$$\lambda_j = \sum_{i=1}^{n} \alpha_{ij}\mu_i.$$

Artin's lemma on the independence of characters, [3] Theorem 4.1, now implies that each λ_j is 0, and since the μ_i are linearly independent over K, it follows that $\alpha_{ij} = 0$ for all i and j. Thus the elements $\mu_i\sigma_j$ are linearly independent over K and this proves that E does indeed equal $\mathrm{End}_K(L)$. □

Theorem 1 can be interpreted in terms of a skew group algebra construction. See, for example, Theorem 31.6 of [4]. Some implications of the theorem when the Galois group G is cyclic are derived in [2].

3. Endomorphisms of rank 1 and trace functions

Let U be a K-subspace of L. The subset of all elements τ of $\mathrm{End}_K(L)$ that satisfy $\tau(U) = 0$ is a subspace of $\mathrm{End}_K(L)$ and it is easy to prove that it has dimension $n(n - \dim_K U)$. Endomorphisms in this subspace have rank at most $n - \dim_K U$.

We recall that a *K-hyperplane* in L is a K-subspace of dimension $n - 1$. We provide a proof now of a well-known fact concerning K-hyperplanes. (Note that the argument below applies to arbitrary extensions of K of finite degree, not just Galois extensions.)

Lemma 1. *Let H be a K-hyperplane in L. Then every K-hyperplane in L has the form $a^{-1}H$ for some non-zero $a \in L$.*

Proof. Let L^* denote the dual space of L, that is, the vector space of K-linear mappings of L into K. It is easy to see that each K-hyperplane arises as the kernel of a non-zero element of L^*, and thus there exists some $g \in L^*$ such that $H = \ker g$. Now given $a \in L$, we can define $g^a \in L^*$ by

$$g^a(x) = g(ax),$$

for all $x \in L$. Then (provided $a \neq 0$)

$$\ker g^a = a^{-1} \ker g = a^{-1}H.$$

We easily check that the function from L to L^* sending a to g^a is a monomorphism of K-vector spaces, and hence an isomorphism, since

$$\dim_K L = \dim_K L^* = n.$$

Since, as we observed above, each K-hyperplane is the kernel of a non-zero element of L^*, the result follows. □

The standard example of a K-hyperplane in L is the *trace zero* hyperplane H_0, which is the kernel of the trace form $\mathrm{Tr} = \mathrm{Tr}_K^L \in L^*$ defined by

$$\mathrm{Tr}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

If we consider the element

$$\pi = \sigma_1 + \cdots + \sigma_n$$

in $\mathrm{End}_K(L)$, it is clear that $H_0 = \ker \pi$. (Note that we are using the two notations Tr and π for the trace function. We use π when we think of the trace function as an element of $\mathrm{End}_K(L)$.)

Suppose now that H is some other K-hyperplane in L. We know from Lemma 1 that $H = a^{-1}H_0$ for some $a \in L$.

Lemma 2. *Suppose that H is the K-hyperplane $a^{-1}H_0$. Then the element π_a defined by*

$$\pi_a = \sigma_1(a)\sigma_1 + \cdots + \sigma_n(a)\sigma_n$$

in $\mathrm{End}_K(L)$ *annihilates H.*

Proof. This is an immediate consequence of the facts that π annihilates H_0 and the σ_i are automorphisms of L. □

We observe here that any endomorphism which annihilates H is an L-multiple of π_a, since the set of all such multiples of π_a is an n-dimensional K-subspace of $\mathrm{End}_K(L)$ and the subspace of all endomorphisms annihilating H is also n-dimensional.

We have therefore obtained the following characterization of elements of rank 1 in $\mathrm{End}_K(L)$.

Theorem 2. *The elements of rank* 1 *in* $\mathrm{End}_K(L)$ *are precisely those of the form*

$$\lambda\pi_a = \lambda\sigma_1(a)\sigma_1 + \cdots + \lambda\sigma_n(a)\sigma_n,$$

where λ and a are non-zero elements of L.

The product of two endomorphisms of rank 1 clearly is either 0 or else has rank 1. We can obtain a formula for such a product using the representation of rank 1 endomorphisms given in Theorem 2.

Theorem 3. *Let λ, μ, a and b be non-zero elements of L and let $\lambda\pi_a$, $\mu\pi_b$ be corresponding elements of rank* 1 *in* $\mathrm{End}_K(L)$. *Then we have*

$$(\lambda\pi_a)(\mu\pi_b) = \lambda\mathrm{Tr}(a\mu)\pi_b.$$

Hence the product is 0 *if and only if* $\mathrm{Tr}(a\mu) = 0$, *and $\mu\pi_b$ is an idempotent when* $\mathrm{Tr}(b\mu) = 1$.

Proof. By definition,

$$(\lambda\pi_a)(\mu\pi_b) = \left(\sum_{\sigma\in G}\lambda\sigma(a)\sigma\right)\left(\sum_{\tau\in G}\mu\tau(b)\tau\right) = \sum_{\sigma,\tau\in G}\lambda\sigma(a)\sigma(\mu)\sigma\tau(b)\sigma\tau.$$

Fixing an element ρ in G, we see that the coefficient of ρ in the product above is

$$\sum_{\sigma\in G}\lambda\sigma(a)\sigma(\mu)\rho(b) = \lambda\mathrm{Tr}(a\mu)\rho(b).$$

It follows that

$$(\lambda\pi_a)(\mu\pi_b) = \lambda\mathrm{Tr}(a\mu)\pi_b.$$

The other statements relating to the trace are clear from this formula. □

Given an element τ of $\mathrm{End}_K(L)$, let $\mathrm{tr}(\tau)$ denote the usual (matrix-theoretic) trace of τ. When τ has rank 1, it is straightforward to see that

$$\tau^2 = \mathrm{tr}(\tau)\tau.$$

Thus taking $\lambda\pi_a = \mu\pi_b$ in Theorem 3, we obtain the following result on the trace of any endomorphisms of rank 1.

Corollary 1. *Let λ and a be non-zero elements of L and let $\lambda\pi_a$ be the corresponding element of rank 1 in $\mathrm{End}_K(L)$. Then we have*

$$\mathrm{tr}(\lambda\pi_a) = \mathrm{Tr}(\lambda a).$$

Corollary 1 establishes a relationship between the matrix-theoretic trace and the field-theoretic trace. We proceed to give complete information on this topic by showing that any endomorphism can be expressed as an L-linear combination of rank 1 elements of the form π_a. We require the following well-known result, for which we supply a proof.

Lemma 3. *Let $x_1, \ldots, x_n$ be a K-basis for L. Then the $n \times n$ matrix B whose i, j entry is $\sigma_j(x_i)$ is invertible.*

Proof. Suppose by way of contradiction that B is not invertible. Then L contains scalars $\lambda_1, \ldots, \lambda_n$, not all 0, such that

$$\lambda_1\sigma_1(x_i) + \cdots + \lambda_n\sigma_n(x_i) = 0$$

for $1 \leqslant i \leqslant n$. Let x be any element of L. We can write

$$x = \mu_1 x_1 + \cdots + \mu_n x_n$$

for unique elements $\mu_1, \ldots, \mu_n$ in K. Now multiplying the equation above by μ_i, and summing the n equations thus derived, we deduce that

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0.$$

Since x is arbitrary, this contradicts the independence of the σ_i over L. It follows that B is indeed invertible. □

Given a K-basis $x_1, \ldots, x_n$ for L, we set

$$\pi_i = \sigma_1(x_i)\sigma_1 + \cdots + \sigma_n(x_i)\sigma_n$$

for $1 \leqslant i \leqslant n$. We show next that every element of $\mathrm{End}_K(L)$ is an L-linear sum of the n elements π_i.

Lemma 4. *Let $x_1, \ldots, x_n$ be a K-basis for L and let π_i be the elements of $\mathrm{End}_K(L)$ defined above. Let τ be any element of $\mathrm{End}_K(L)$. Then there exist unique elements $\mu_1, \ldots, \mu_n$ in L with*

$$\tau = \mu_1\pi_1 + \cdots + \mu_n\pi_n.$$

Proof. Write

$$\tau = \lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n,$$

where the $\lambda_i \in L$. Then, using the definition of the π_i, we have to find elements μ_i so that

$$\lambda_i = \mu_1\sigma_i(x_1) + \cdots + \mu_n\sigma_i(x_n)$$

for $1 \leqslant i \leqslant n$. This is a system of linear equations whose coefficient matrix is the transpose of the matrix B defined in Lemma 3. Since B is invertible, the system has a unique solution, as required. □

We may interpret Lemma 4 as follows. The set of all L-multiples of the endomorphism π_i is a subspace of $\mathrm{End}_K(L)$ of dimension n, all of whose non-zero elements have rank 1. Then we see that

$\mathrm{End}_K(L)$ is a direct sum of n of these n-dimensional subspaces consisting of rank 1 elements. Of course, such decompositions exist for the algebra of endomorphisms of an n-dimensional vector space over an arbitrary field.

We can now determine the trace of any endomorphism.

Theorem 4. *Let*

$$\tau = \lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n,$$

where $\sigma_1 = 1$, *be any element of* $\mathrm{End}_K(L)$. *Then we have*

$$\mathrm{tr}(\tau) = \mathrm{Tr}(\lambda_1).$$

Proof. By Lemma 4, we may write

$$\tau = \mu_1\pi_1 + \cdots + \mu_n\pi_n.$$

for unique elements $\mu_1, \ldots, \mu_n$ in L. Then we have

$$\mathrm{tr}(\tau) = \sum_{i=1}^{n} \mathrm{tr}(\mu_i\pi_i).$$

Lemma 1 implies that $\mathrm{tr}(\mu_i\pi_i) = \mathrm{Tr}(\mu_i x_i)$ and we deduce from the linearity of Tr that

$$\mathrm{tr}(\tau) = \mathrm{Tr}\left(\sum_{i=1}^{n} \mu_i x_i\right).$$

However, if we compare the coefficient of σ_1 in τ and in $\mu_1\pi_1 + \cdots + \mu_n\pi_n$, we see that

$$\lambda_1 = \mu_1 x_1 + \cdots + \mu_n x_n$$

and the formula for $\mathrm{tr}(\tau)$ follows. □

4. Determinants associated to hyperplanes

We turn to a more detailed study of the matrix B of Lemma 3, and of a related $n-1 \times n-1$ matrix. Lemma 3 implies that $\det B \neq 0$. It must be well-known that $\det B$ is either an element of K or else lies in a quadratic extension of K. As we wish to generalize this fact, we provide a proof.

Let σ be any element of G and let $\sigma(B)$ be the matrix obtained from B by applying σ to its entries. As G is a group, it is clear that the columns of $\sigma(B)$ are obtained by permuting those of B according to the regular permutation action of σ on G by left multiplication. Thus if $\epsilon(\sigma)$ denotes the sign of σ acting on G by left multiplication, we have

$$\sigma(\det B) = \det \sigma(B) = \epsilon(\sigma) \det B.$$

(If K has characteristic 2, the sign function is trivial.)

We need to recall when the sign function ϵ of the regular permutation representation of G is non-trivial. This occurs precisely when K has characteristic different from 2, G has even order and its Sylow 2-subgroups are cyclic. Suppose then that K has characteristic different from 2, G has even order and a cyclic Sylow 2-subgroup. Elementary theory shows that G has a normal 2-complement and hence a unique subgroup of index 2. In this case, L contains a unique extension of K of degree 2, $K(\alpha)$, say, where $\alpha^2 \in K$. We can therefore state the following result.

Theorem 5. *Let L be a Galois extension of K of degree n with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. Let $x_1, \ldots, x_n$ be a K-basis of L. Then the $n \times n$ matrix B whose i, j entry is $\sigma_j(x_i)$, $1 \leqslant i, j \leqslant n$, is invertible. Furthermore,*

$$\det B \in K$$

if K has characteristic 2 or if the Sylow 2-subgroup of G is not cyclic. If K has characteristic different from 2 and G has a cyclic Sylow 2-subgroup,

$$\det B = \mu\alpha,$$

where $\mu \in K$, $\alpha^2 \in K$ and $K(\alpha)$ is the unique quadratic extension of K contained in L.

We wish to obtain an analogue of Theorem 5 using an $n-1 \times n-1$ matrix formed from a basis of the trace zero hyperplane H_0.

Let $b_2, \ldots, b_n$ be a K-basis of H_0. We may extend this basis of H_0 to a basis of L by adjoining any element b_1, say, outside H_0. Let E be the $n \times n$ matrix whose i, j entry is $\sigma_j(b_i)$. Given any element x of L, let $E(x)$ be the $n \times n$ matrix obtained by replacing the first row of E by the row $\sigma_1(x), \ldots, \sigma_n(x)$. (Thus $E(b_1)$ is the original E.)

We now define an element θ of $\mathrm{End}_K(L)$ by setting

$$\theta(x) = \det E(x).$$

We note that $\theta(b_1) = \det E \neq 0$, by Lemma 3, so that $\theta \neq 0$. On the other hand, if x is in H_0, it is a K-linear combination of $b_2, \ldots, b_n$ and hence elementary properties of determinants imply that $\det E(x) = 0$. It follows that θ vanishes on H_0 and is therefore an L-multiple of π.

Expanding $\det E(x)$ along its first row, we obtain

$$\theta = \det E_1\, \sigma_1 - \det E_2\, \sigma_2 + \cdots + (-1)^{n-1} \det E_n\, \sigma_n,$$

where E_i is the $n-1 \times n-1$ matrix obtained by omitting the first row and ith column of E.

By the earlier argument, for each element σ of G, we have

$$\sigma(\det E(x)) = \det \sigma(E(x)) = \epsilon(\sigma) \det E(x),$$

where ϵ is the sign function of the regular representation of G.

Recalling that we have chosen σ_1 to be the identity of G, it is straightforward to see that for $1 \leqslant i \leqslant n$, $\sigma_i(E_1)$ is obtained by a permutation of the columns of E_i. Thus we have

$$\sigma_i(\det E_1) = \det \sigma_i(E_1) = \epsilon_i \det E_i,$$

where $\epsilon_i = \pm 1$. We observe that this implies that $\det E_1 \neq 0$, since otherwise $\det E_i = 0$ for all i and hence $\theta = 0$, a contradiction.

Lemma 5. *With the notation above, we have*

$$\epsilon_i = (-1)^{i-1}\epsilon(\sigma_i).$$

Proof. For any integer i with $1 \leqslant i \leqslant n$, and any $x \in L$, we have

$$\sigma_i(\det E(x)) = \det(\sigma_i(E(x))) = \epsilon(\sigma_i) \det E(x).$$

We equally well have

$$\sigma_i(\det E(x)) = \sigma_i(\det E_1)\sigma_i\sigma_1(x) + \cdots + (-1)^{n-1}\sigma_i(\det E_n)\, \sigma_i\sigma_n(x).$$

Since the Galois automorphisms are independent over L, comparison of the coefficient of σ_i in these two expressions for $\sigma_i(\det E(x))$ shows that

$$\epsilon(\sigma_i)(-1)^{i-1} \det E_i = \sigma_i(\det E_1) = \epsilon_i \det E_i.$$

The result follows, since $\det E_i \neq 0$. □

Lemma 5 implies that

$$\theta = \epsilon(\sigma_1)\sigma_1(\det E_1)\sigma_1 + \cdots + \epsilon(\sigma_n)\sigma_n(\det E_1)\sigma_n.$$

Next, we relate π and θ.

Corollary 2. *With the notation previously introduced, we have*

$$(\det E_1)\pi = \theta$$

and hence

$$\det E_1 = \epsilon(\sigma_i)\sigma_i(\det E_1)$$

for $1 \leqslant i \leqslant n$.

Proof. As we observed, π and θ are L-multiples of each other. It is easy to check that $(\det E_1)\pi$ and θ have the same coefficient of $\sigma_1 = 1$, and therefore they must be equal. □

We obtain the following analogue of Theorem 5.

Theorem 6. *Let L be a Galois extension of K of degree n with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$, where $\sigma_1 = 1$. Let H_0 be the trace zero K-hyperplane in L. Let $b_2, \ldots, b_n$ be a K-basis of H_0. Then the $n-1 \times n-1$ matrix E_1 whose i, j entry is $\sigma_j(b_i)$, $2 \leqslant i, j \leqslant n$, is invertible. Furthermore,*

$$\det E_1 \in K$$

if K has characteristic 2 or if the Sylow 2-subgroup of G is not cyclic. If K has characteristic different from 2 and G has a cyclic Sylow 2-subgroup,

$$\det E_1 = \kappa\alpha,$$

where $\kappa \in K$, $\alpha^2 \in K$ and $K(\alpha)$ is the unique quadratic extension of K contained in L.

We note that, while we formed E_1 by omitting the specific automorphism $\sigma_1 = 1$, we would obtain the same result for any analogue of E_1 formed by omitting exactly one automorphism in G.

We conclude this section by observing that a version of Theorem 6 holds for any hyperplane. Let H be a K-hyperplane in L. We know from Lemma 1 that $H = a^{-1}H_0$ for some non-zero $a \in L$. Thus if $b_2, \ldots, b_n$ is a K-basis of H_0,

$$c_2 = a^{-1}b_2, \ldots, c_n = a^{-1}b_n$$

is a K-basis of H. Let C_1 be the $n-1 \times n-1$ matrix whose i, j entry is $\sigma_j(c_i)$, $2 \leqslant i, j \leqslant n$. It is straightforward to see that

$$\det C_1 = \sigma_2(a^{-1}) \cdots \sigma_n(a^{-1}) \det E_1.$$

But since $\sigma_1(a^{-1}) = a^{-1}$ and

$$\sigma_1(a^{-1})\sigma_2(a^{-1}) \cdots \sigma_n(a^{-1}) \in K,$$

we see that

$$\det C_1 = a\lambda \det E_1$$

for some non-zero $\lambda \in K$. We therefore have the following result.

Theorem 7. *Let L be a Galois extension of K of degree n with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$, where $\sigma_1 = 1$. Let H_0 be the trace zero K-hyperplane in L and let H be any other K-hyperplane in L. Let $c_2, \ldots, c_n$ be a K-basis of H_0. Then the $n-1 \times n-1$ matrix C_1 whose i, j entry is $\sigma_j(c_i)$, $2 \leqslant i, j \leqslant n$, is invertible. Furthermore,*

$$H = (\det C_1)^{-1}(H_0)$$

if K has characteristic 2 or if the Sylow 2-subgroup of G is not cyclic. If K has characteristic different from 2 and G has a cyclic Sylow 2-subgroup,

$$H = \alpha(\det C_1)^{-1}(H_0),$$

where $\kappa \in K$, $\alpha^2 \in K$ and $K(\alpha)$ is the unique quadratic extension of K contained in L.

5. Cyclic extensions and annihilating elements

We now concentrate on the case that G is a *cyclic* group (in which case we say that L is a cyclic extension of K).

Let σ be a generator of G. Changing notation slightly, Theorem 1 implies that each element of $\mathrm{End}_K(L)$ is expressible in the form

$$\mu_{n-1}\sigma^{n-1} + \cdots + \mu_1\sigma + \mu_0 I$$

for unique $\mu_0, \ldots, \mu_{n-1}$ in L. We may thus think of the elements of $\mathrm{End}_K(L)$ as polynomials in σ with entries in L.

We proved the following independence criterion for elements of L in [1], Theorem 4.

Theorem 8. *Let L be a cyclic Galois extension of K of degree n and suppose that σ generates the Galois group of L over K. Let k be an integer satisfying $1 \leqslant k \leqslant n$ and let*

$$b_1, \ldots, b_k$$

be elements of L.

Then these elements are linearly dependent over K if and and only if

$$\det S = 0,$$

where S is the $k \times k$ matrix S whose i, j entry is $\sigma^{j-1}(b_i)$, $1 \leqslant i, j \leqslant k$.

(Note that we are expressing the result using the transpose of the matrix described in [1].)

As a consequence of this result, we obtained the following theorem concerning endomorphisms which annihilate a given subspace.

Theorem 9. *Let L be a cyclic Galois extension of K of degree n and suppose that σ generates the Galois group of L over K. Let k be an integer satisfying $1 \leqslant k \leqslant n$ and let U be a subspace of L of dimension k. Then there exists a unique monic polynomial w, say, of degree k in $L[t]$ such that*

$$U = \{x \in L : w(\sigma)x = 0\}.$$

Using some of the ideas developed in Section 3, we now show that the polynomial w above can be expressed (in principle) using determinants. Let U be a subspace of L of dimension k and let $b_1, \ldots, b_k$ be a K-basis of U. Let x be an arbitrary element of L and let $D(x)$ be the $k+1 \times k+1$ matrix whose first row has entries

$$\sigma^{j-1}(x), \quad 1 \leqslant j \leqslant k+1$$

and whose ith row has entries

$$\sigma^{j-1}(b_{i-1}), \quad 2 \leqslant i \leqslant k+1,\ 1 \leqslant j \leqslant k+1.$$

We define an element ϕ of $\mathrm{End}_K(L)$ by setting

$$\phi(x) = \det D(x).$$

The arguments of Section 2 imply that ϕ vanishes on U. Expanding $\det D(x)$ along its first row, we obtain

$$\phi = \det D_1 - \det D_2\, \sigma + \cdots + (-1)^k \det D_{k+1}\, \sigma^k,$$

where D_i is the $k \times k$ matrix obtained by omitting the first row and ith column of $D(x)$. Note that $\det D_{k+1} \neq 0$ by Theorem 8. We therefore obtain the following description of the polynomial in Theorem 9.

Theorem 10. *The polynomial w described in Theorem 9 is*

$$t^k - \det(D_k D_{k+1}^{-1})t^{k-1} + \cdots + (-1)^k \det(D_1 D_{k+1}^{-1}),$$

where the $k \times k$ matrices D_i are defined above. Moreover, since $D_1 = \sigma(D_{k+1})$, the constant term has the form $(-1)^k a\sigma(a)^{-1}$, for some element a of L.

We have seen that the elements of $\mathrm{End}_K(L)$ may be expressed as polynomials in σ, with the relation $\sigma^n = 1$ holding. To avoid possible confusion with ordinary polynomial multiplication, we shall let $f(\sigma) * g(\sigma)$ denote the product in $\mathrm{End}_K(L)$ of two such polynomial expressions. We have the basic rule

$$(\lambda\sigma^i) * (\mu\sigma^j) = \lambda\sigma^i(\mu)\sigma^{i+j}$$

whenever λ and μ are elements of L.

Let $f(t)$ and $g(t)$ be polynomials in $L[t]$ of degree r and s, respectively. Since the elements $\sigma^0 = 1, \sigma, \ldots, \sigma^{n-1}$ are linearly independent over L, it follows that

$$f(\sigma) * g(\sigma) \neq 0$$

provided that $r + s < n$.

Definition 1. Let U be a K-subspace of L. We denote the monic polynomial of degree $\dim U$ in Theorem 9 by $m_U(t)$.

Lemma 6. *Let U be a proper K-subspace of L. Each element of* $\mathrm{End}_K(L)$ *which annihilates U may be uniquely expressed in the form*

$$f(\sigma) * m_U(\sigma),$$

where $f(t) \in L[t]$ *has degree at most* $n - \dim U - 1$.

Proof. Let $k = \dim U$. We have observed that the subspace of $\mathrm{End}_K(L)$ which annihilates U has dimension $n(n-k)$. Let $f(t)$, $g(t)$ be any two different polynomials in $L[t]$ of degree at most $n-k-1$. It is clear that both $f(\sigma) * m_U(\sigma)$ and $g(\sigma) * m_U(\sigma)$ annihilate U. Moreover,

$$f(\sigma) * m_U(\sigma) \neq g(\sigma) * m_U(\sigma),$$

since $(f(\sigma) - g(\sigma)) * m_U(\sigma) \neq 0$.

The set of all elements of $\mathrm{End}_K(L)$ of the form $f(\sigma) * m_U(\sigma)$, where $\deg f(t) \leqslant n-k-1$, is thus a K-vector space of dimension $n(n-k)$ and hence coincides with the subspace of $\mathrm{End}_K(L)$ which annihilates U, as required. □

Continuing with the notation above, let W be a subspace of U of dimension $k-1$. Certainly, $m_U(\sigma)$ annihilates W and hence

$$m_U(\sigma) = f(\sigma) * m_W(\sigma),$$

for some monic polynomial $f(t) \in L[t]$, by Lemma 6. A comparison of degrees shows that $f(t)$ is linear and thus has the form $t - a$ for some $a \in L$. We will now demonstrate how a may be calculated.

Theorem 11. *Let* U *be a proper* K*-subspace of* L *of dimension* k *and let* W *be a subspace of* U *of codimension* 1. *Let* $b_1, \ldots, b_{k-1}$ *be a* K*-basis of* W *and let* b_k *be any element of* U *not in* W. *Let* D_1 *and* D_{k+1} *be the* $k \times k$ *matrices formed using the basis* $b_1, \ldots, b_k$ *of* U, *as described in Theorem 10, and let* C_1, C_k *be the corresponding* $k-1 \times k-1$ *matrices formed by using the basis* $b_1, \ldots, b_{k-1}$ *of* W. *Then we have the factorization*

$$m_U(\sigma) = (\sigma - a) * m_W(\sigma),$$

where

$$a = \det(D_1 D_{k+1}^{-1}) \det(C_1^{-1} C_k).$$

Proof. This follows from using the explicit forms of the constant terms in the polynomials $m_U(t)$ and $m_W(t)$ in Theorem 10. □

Our final result, expressing $m_U(\sigma)$ as a product of k terms of the form $\sigma - a$, follows by induction.

Corollary 3. *Let* U *be a proper* K*-subspace of* L *of dimension* k. *Then there is a factorization*

$$m_U(\sigma) = (\sigma - a_1) * \cdots * (\sigma - a_k)$$

in $\mathrm{End}_K(L)$, *where each element* a_i *has the form* $b_i \sigma(b_i)^{-1}$ *for suitable* $b_i \in L$.

Acknowledgments

The authors wish to thank the referee for helpful suggestions.

References

[1] R. Gow, R. Quinlan, Galois extensions and subspaces of alternating bilinear forms with special rank properties, submitted for publication.
[2] R. Gow, G. McGuire, J. Sheekey, Properties of subspaces of endomorphisms with special rank properties, preprint, 11 pages.
[3] S. Lang, Algebra, third ed., Addison-Wesley, Reading, Mass, 1993.
[4] D.S. Passman, Infinite Crossed Products, Academic Press, Inc., Boston, San Diego, New York, 1989.